## REMARKS

In response to the Office Action, Applicant has amended the pending claims to better define Applicant's invention. The claims now pending are claims 1, 3-5, 12-14, and 18-32; claims 31 and 32 have been added by this Amendment.

Within the Office Action, the Examiner rejected claims 1-30 as originally filed under 35 U.S.C. §102(e) as describing subject matter purportedly anticipated by U.S. Patent No. 6,243,468 to Pearce, et al. ("Pearce"). Applicant respectfully requests the Examiner to reconsider such rejection, and to reexamine the present application in view of the above claim amendments in light of the following remarks.

Independent claim 1 as amended recites a method of preventing piracy of a given software application which requires that a user enter personal data that identifies the user, and to communicate user data over a communications network with a remote service system, wherein the user data is derived, at least in part, from the personal data that identifies the user, and derived, at least in part, from a unique identification code assigned to a particular copy of the software application. Claim 1 further recites the step of selectively transmitting service data to the user's computer from the remote service system when the remote service system determines that such service data should be transmitted. These steps are not disclosed or suggested by the cited Pearce patent.

Pearce discloses that the software application installed on the user's computer generates a hardware ID based upon hardware components installed in the computer running such software. This hardware ID is not derived from personal information that identifies the user; rather, it is based upon characteristics of hardware components that are installed in the user's machine. Pearce's method concatenates the hardware ID and a product ID for communication to a registration authority. The registration authority sends back a registration ID. The software on the user's computer system saves this registration ID on the user's computer system. Each time the user launches the software application, the software generates a test ID (based upon the product ID and current hardware ID) for comparison to the registration ID previously obtained from the

registration authority. If they match, operation continues; if they do not match, operation of the software halts.

Thus, in Pearce, the user obtains the registration ID from the registration authority without submitting any personal user data. Moreover, in Pearce, the software application on the user's computer runs a test each time that the software is launched. In contrast, in the method of claim 1, the user must submit personal identifying data to the remote service computer, and the determination of whether the software is pirated is made by the remote service computer, and not by the user's computer.

The differences between the claimed method and Pearce's system are significant. If a user buys a new computer and desires to transfer the contents of his old hard drive (including a software application protected by the Pearce scheme) to his new hard drive in the new computer, Pearce's anti-piracy system will not allow the software to operate on the new computer because the hardware ID will now be entirely different; this is true even though the user has properly paid for a license to use such software, and even if the user deletes the software from his old computer. In contrast, under the system of method claim 1, the user's new computer will continue to run the software application because the service data previously obtained is already stored on the user's hard drive. Even if the user decides to re-install the software application onto the new computer from scratch, the user's new computer can communicate with the remote service computer, provide the relevant user data, including data that personally identifies the user, and once again obtain the required service data. So long as the user data (including the user's personal data) matches that previously archived by the remote service computer for this particular copy of the software application, there is no immediate concern of piracy, and the required service data will be provided to the user over the communications network.

Claim 23 as amended is directed to a system for preventing piracy of a given software application including a user computer system on which a user desires to operate the software application, and a remote service computer system coupled to the user computer system via a communications network. The user computer transmits user data to the remote service computer, wherein the user data is derived at least in part from personal data entered by the user which

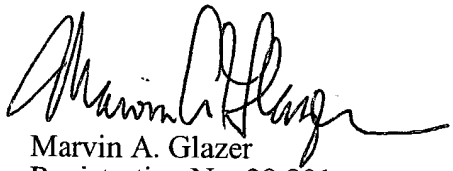
identifies the user, and at least in part from a unique identification code. The remote service computer receives and stores such user data, and transmits required service data to the user computer system over said communications network when the remote service computer system determines that said user is not pirating said software application. Dependent claim 24 further explains that such determination may be made by the remote service computer system by comparing user data received from the user computer system to user data previously archived by the remote service computer relative to the same unique identification code to ensure that user data received by the remote service computer is consistent with user data previously archived by the remote service computer for a given unique identification code. As explained above, Pearce does not utilize user data derived from personal data that identifies a particular user. Likewise, Pearce does not use the remote service computer to determine whether or not to transmit service data (or a registration ID) to the user's computer.

New independent claim 31 recites a method of preventing piracy of a given software application similar to the method of amended claim 1, except that claim 31 does not recite the step of comparing user data to previously archived data. However, like method claim 1, new claim 31 requires the user to transmit user data to a remote service computer wherein the user data is derived at least in part from personal data that identifies the user. As noted above, this method is not disclosed or suggested by Pearce. The step of archiving received user data, and using such archived data when comparing received user data for each unique identification code, in order to determine whether a user is pirating the software application, is addressed in new dependent claim 32.

In light of the amendments to the claims, and in view of the arguments set forth above, Applicant submits that the pending claims are not anticipated or suggested by the prior art of record, and that the present application is now in condition for allowance, which action is earnestly requested.

Respectfully submitted,

CAHILL, VON HELLENS & GLAZER P.L.C.



Marvin A. Glazer
Registration No. 28,801

155 Park One
2141 East Highland Avenue
Phoenix, Arizona 85016
Ph. (602) 956-7000
Fax (602) 495-9475
Docket No. 6589-A-5